

## CLAIMS

- 1 1. (Original) A method for managing access to data in a database subject to a plurality of  
2 label-based security policies, the method comprising the steps of:  
3 receiving, within a database management system, a request for performing an operation  
4 set of one or more operations on data in a table of the database;  
5 determining which policies, of the plurality of label-based policies, apply to the table  
6 based on a policy set of one or more policies associated with the table; and  
7 for each operation in the operation set, determining whether to perform the operation on a  
8 row of the table based on a set of labels associated with the row, the set of labels  
9 corresponding to the policy set.
- 1 2. (Original) A method according to Claim 1, further comprising adding a policy column to  
2 the table for each policy in the policy set associated with the table
- 1 3. (Original) A method according to Claim 2, further comprising storing a label, of the set  
2 of labels associated with the row, in a corresponding policy column of the row.
- 1 4. (Original) A method according to Claim 2, said step of determining which policies apply  
2 further comprising the step of determining whether a column is a policy column.
- 1 5. (Original) A method according to Claim 1, wherein the policy set associated with the  
2 table includes two or more policies of the plurality of label-based policies.
- 1 6. (Previously Presented) A method for managing access to data in a database based on a  
2 database policy set of one or more label-based security policies, the method comprising  
3 the steps of:  
4 registering, with a database management system, one or more packages of routines,

5            wherein each package of said one or more packages implements a security model  
6            that supports a model set of one or more policies of the database policy set and  
7            said each package includes an access mediation routine;  
8            associating a first policy of a first model set in a first package with a first table within the  
9            database system; and  
10           invoking the access mediation routine in the first package for determining whether to  
11           allow operation on data in the first table based on the first policy.

1    7.    (Previously Presented) A method according to Claim 6, further comprising the step of  
2           forming said each package of said one or more packages so that the access mediation  
3           routine conforms to a specified interface for enforcing a policy in the database  
4           management system.

1    8.    (Previously Presented) A method according to Claim 7, said step of forming said each  
2           package further comprising including one or more administrative routines for defining a  
3           policy for the model set.

1    9.    (Original) A method according to Claim 8, said step of including one or more  
2           administrative routines for defining a policy further comprising including one or more  
3           administrative routines for defining a name for a particular policy; labels for the  
4           particular policy; descriptions for the labels; and properties for the labels.

1    10.   (Original) A method according to Claim 6, further comprising the step of invoking an  
2           administrative routine of the first package for defining the first policy.

1    11.   (Previously Presented) A method according to Claim 10, said step of invoking the  
2           administrative routine of the first package further comprising providing to the

3 administrative routine of the first package a plurality of parameters including a policy  
4 name for the first policy and a plurality of label names for labels of the first policy.

1 12. (Original) A method according to Claim 6, further comprising, in response to attempts to  
2 operate on data in a row in the table, the step of determining that the first policy applies  
3 to the table.

1 13. (Original) A method according to Claim 6, further comprising the steps of:  
2 associating a second policy of a second model set in a second package with a second  
3 table within the database system; and  
4 invoking the access mediation routine in the second package for determining whether to  
5 allow operation on data in the second table based on the second policy.

1 14. (Original) A method according to Claim 13, wherein the second model in the second  
2 package is the same as the first model in the first package.

1 15. (Original) A method according to Claim 13, wherein the second model in the second  
2 package is different from the first model in the first package.

1 16. (Original) A method according to Claim 13, wherein the second table is the same as the  
2 first table.

1 17. (Original) A method according to Claim 13, wherein the second table is different from  
2 the first table.

1 18. (Original) A method according to Claim 6, said step of invoking the access mediation  
2 routine in the first package further comprising providing data indicating the first policy to  
3 the access mediation routine.

1 19. (Previously Presented) A method according to Claim 6, wherein.  
2 the method further comprises the step of determining a set of allowed labels for the first  
3 policy for a user of the database management system;  
4 said step of invoking the access mediation routine is performed during said step of  
5 determining the set of allowed labels; and  
6 the user is allowed to operate on the data according to the first policy if the data is  
7 associated with a label for the first policy and the label is included in the set of  
8 allowed labels for the first policy.

1 20. (Original) A method according to Claim 19, further comprising the step of storing the set  
2 of allowed labels in a session cache for a communication session between the database  
3 management system and the user.

1 21. (Original) A computer-readable medium carrying one or more sequences of instructions  
2 for managing access to data in a database subject to a plurality of label-based security  
3 policies, wherein execution of the one or more sequences of instructions by one or more  
4 processors causes the one or more processors to perform the steps of:  
5 receiving a request for performing an operation set of one or more operations on data in a  
6 table of the database;  
7 determining which policies, of the plurality of label-based policies, apply to the table  
8 based on a policy set of one or more policies associated with the table; and  
9 for each operation in the operation set, determining whether to perform the operation on a  
10 row of the table based on a set of labels associated with the row, the set of labels

11 corresponding to the policy set.

1 22. (Original) A computer-readable medium according to Claim 21, wherein execution of the  
2 one or more sequences of instructions further causes the one or more processors to  
3 perform the step of adding a policy column to the table for each policy in the policy set  
4 associated with the table

1 23. (Original) A computer-readable medium according to Claim 22, wherein execution of the  
2 one or more sequences of instructions further causes the one or more processors to  
3 perform the step of storing a label, of the set of labels associated with the row, in a  
4 corresponding policy column of the row.

1 24. (Original) A computer-readable medium according to Claim 22, said step of determining  
2 which policies apply further comprising the step of determining whether a column is a  
3 policy column.

1 25. (Original) A computer-readable medium according to Claim 21, wherein the policy set  
2 associated with the table includes two or more policies of the plurality of label-based  
3 policies.

1 26. (Previously Presented) A computer-readable medium carrying one or more sequences of  
2 instructions for managing access to data in a database based on a database policy set of  
3 one or more label-based security policies, wherein execution of the one or more  
4 sequences of instructions by one or more processors causes the one or more processors to  
5 perform the steps of:  
6 registering, with a database management system, one or more packages of routines,  
7 wherein each package of said one or more packages implements a security model

- 8           that supports a model set of one or more policies of the database policy set and  
9           said each package includes an access mediation routine;  
10          associating a first policy of a first model set in a first package with a first table within the  
11          database system; and  
12          invoking the access mediation routine in the first package for determining whether to  
13          allow operation on data in the first table based on the first policy.
- 1   27.   (Original) A computer-readable medium according to Claim 26, wherein the access  
2          mediation routine conforms to a specified interface for enforcing a policy in the database  
3          management system.
- 1   28.   (Previously Presented) A computer-readable medium according to Claim 27, wherein  
2          said each package of said one or more packages includes one or more administrative  
3          routines for defining a policy for the model set.
- 1   29.   (Original) A computer-readable medium according to Claim 28, wherein execution of the  
2          one or more sequences of instructions further causes the one or more processors to  
3          perform the step of defining a name for a particular policy; labels for the particular  
4          policy; descriptions for the labels; and properties for the labels.
- 1   30.   (Original) A computer-readable medium according to Claim 26, wherein execution of the  
2          one or more sequences of instructions further causes the one or more processors to  
3          perform the step of invoking an administrative routine of the first package for defining  
4          the first policy.

- 1 31. (Previously Presented) A computer-readable medium according to Claim 30, said step of  
2 invoking the administrative routine of the first package further comprising providing to  
3 the administrative routine of the first package a plurality of parameters including a policy  
4 name for the first policy and a plurality of label names for labels of the first policy.
- 1 32. (Original) A computer-readable medium according to Claim 26, wherein execution of the  
2 one or more sequences of instructions further causes the one or more processors to  
3 perform, in response to attempts to operate on data in a row in the table, the step of  
4 determining that the first policy applies to the table.
- 1 33. (Original) A computer-readable medium according to Claim 26, wherein execution of the  
2 one or more sequences of instructions further causes the one or more processors to  
3 perform the steps of:  
4 associating a second policy of a second model set in a second package with a second  
5 table within the database system; and  
6 invoking the access mediation routine in the second package for determining whether to  
7 allow operation on data in the second table based on the second policy.
- 1 34. (Original) A computer-readable medium according to Claim 33, wherein the second  
2 model in the second package is the same as the first model in the first package.
- 1 35. (Original) A computer-readable medium according to Claim 33, wherein the second  
2 model in the second package is different from the first model in the first package.
- 1 36. (Original) A computer-readable medium according to Claim 33, wherein the second table  
2 is the same as the first table.

- 1 37. (Original) A computer-readable medium according to Claim 33, wherein the second table  
2 is different from the first table.
- 1 38. (Original) A computer-readable medium according to Claim 26, said step of invoking the  
2 access mediation routine in the first package further comprising providing data indicating  
3 the first policy to the access mediation routine.
- 1 39. (Previously Presented) A computer-readable medium according to Claim 26, wherein.  
2 execution of the one or more sequences of instructions further causes the one or more  
3 processors to perform the step of determining a set of allowed labels for the first  
4 policy for a user of the database management system;  
5 said step of invoking the access mediation routine is performed during said step of  
6 determining the set of allowed labels; and  
7 the user is allowed to operate on the data according to the first policy if the data is  
8 associated with a label for the first policy and the label is included in the set of  
9 allowed labels for the first policy.
- 1 40. (Original) A computer-readable medium according to Claim 39, wherein execution of the  
2 one or more sequences of instructions further causes the one or more processors to  
3 perform the step of storing the set of allowed labels in a session cache for a  
4 communication session between the database management system and the user.